



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/515,384	02/29/2000	Mary Ellen Zurko	C99021US	1649

22879 7590 06/02/2005

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER

DARROW, JUSTIN T

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 06/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/515,384

Applicant(s)

ZURKO ET AL.

Examiner

Justin T. Darrow

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 11 February 2005.
2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 21-27 and 29-41 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5) ☒ Claim(s) 21-27, 29, 30 and 35-41 is/are allowed.
6) ☒ Claim(s) 31 and 32 is/are rejected.
7) ☒ Claim(s) 33 and 34 is/are objected to.
8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
10) ☒ The drawing(s) filed on 22 April 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-41 have been presented for examination. Claims 1-20 have been canceled and new claims 21-28 have been added in a preliminary amendment filed 02/29/2000. Claim 28 has been canceled in an amendment filed 04/22/2004. Claims 21 and 24-27 have been amended and new claims 29-40 have been added in an amendment filed 09/17/2004. Claims 21 and 30-32 have been amended and new claim 41 has been added in an amendment filed 02/11/2005. Claims 21-27 and 29-41 have been examined.

Priority

2. Acknowledgment is made that the instant application is a division of Application No. 07/479,666, filed 02/13/1990, now U.S. Patent No. 6,507,909 B1.

Drawings

3. The drawings were received on 04/22/2004. These drawings are approved.

Response to Arguments

4. Applicant's arguments, see Remarks, page 7, line 17 – page 14, line 9, filed 02/11/2005, with respect to claims 21-26 and 35-41; and claims 27, 29, and 30 have been fully considered and are persuasive. The rejections of claims 21, 23-26, 36, 38, and 40 under 35 U.S.C. 102(e) as being anticipated by Rosenthal, U.S. Patent No. 5,073,933 A, the rejections of claims 22, 35, 37, and 39 under 35 U.S.C. 103(a) as unpatentable under Rosenthal, U.S. Patent No. 5,073,933 A and further in view of Atalla, U.S. Patent No. 4,315,101 A, and the rejections of claims 27, 29,

Art Unit: 2132

and 30 under 35 U.S.C. 103(a) as unpatentable under Rosenthal, U.S. Patent No. 5,073,933 A in view of Rivest et al., U.S. Patent No. 4,405,829 A have been withdrawn.

5. Applicant's arguments concerning claims 31 and 32, filed 02/11/2005, have been fully considered but they are not persuasive.

First, unamended claims 31 and 32 specifically required an untrusted parsing means for generating a parsed trusted command, as recited in the preamble. The rejection of these claims in the last Office action affords patentable weight to this subject matter and applies prior art to it. See MPEP § 2111.02 and *Eaton Corp. v. Rockwell International Corp.*, 66 USPQ2d 1271, 1278 (Fed. Cir. 2003) (holding that characteristics of processed information signals recited in the preamble, but not in the body of the claim, limits the claimed invention). The amendments to claims 31 and 32 moving this subject matter from the preamble to the body of the claim do not change the constructions of these claims. *Id.*

Second, the authorization means in Rosenthal, U.S. Patent No. 5,073,933 A, is the server that receives the credential encrypted with the server's public key (see column 4, lines 19-26). The rejections of claims 31 and 32 characterize the server as only trusted, not untrusted. In fact, claims 31 and 32 do not recite a trusted means. In response to applicant's argument that the reference fails to show a certain feature of applicant's invention, it is noted that the feature upon which applicant relies (i.e., trusted means) is not recited in the rejected claim. Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993). Although claims 31 and 32 do not recite a trusted means, they do incorporate a trusted command.

Art Unit: 2132

When the credential in Rosenthal is successfully decrypted with the server's public key, the verifier in the credential is successfully decrypted with the client's public key, and the credential is successfully checked against a network-wide database to determine the authorization of the particular user (see column 4, lines 24-32), the credential is a trusted command as recited in claims 31 and 32.

Third, the server is a trusted, as discussed above, and the client is untrusted (see column 4, lines 30-31; the client is be operated by a user that may not be authorized with respect to the server). The applicant does not explain how the credential cannot be parsed if it is encrypted (see Remarks, page 15, lines 6-7). The ordinary and customary meaning of terms may be evidenced by a dictionary. See MPEP § 2111.01 II and *Tex. Digital Sys., Inc. v. Telegenix, Inc.*, 308 F.3d 1193, 1202, 64 USPQ2d 1812, 1818 (Fed. Cir. 2002). Here, "parse" is defined as to break input into smaller chunks so that a program can act upon the information (see Microsoft Press Computer Dictionary, 3rd Ed., page 355). Rivest et al., U.S. Patent No. 4,405,829 A describes public key encryption including a conventional blocking means to break a message to be encrypted into message block words before encoding (see column 4, lines 32-37). Because the message is broken into smaller portions so that a program can encrypt it, the message is parsed. Further, Rivest et al. suggest that an encrypted message that underwent being broken up before encoding remains broken up until decryption is completed (see column 4, lines 37-39; following subsequent decoding, the recovered block words may be transformed back to the original message). In contrast to the assertion of the applicant (see Remarks, page 15, lines 9-10), the decryption by the server (see Rosenthal, column 4, lines 24-30) does not include parsing because the parsing in public key encryption occurs at encryption, not decryption. The recitation

Art Unit: 2132

in claims 31 and 32 that an untrusted parsing means for parsing a command is rendered obvious by Rosenthal in view of Rivest et al. by the client encrypting the credential (see Rosenthal, column 4, lines 17-23; the client contacts the server by constructing a credential encrypted with the server's public key) where the message is parsed before encryption (see Rivest et al., column 4, lines 32-37; breaking the message into message block words before encoding) to implement public key encryption for transmission to a particular decoding device (see Rivest et al., column 4, lines 18-22; and see Rosenthal, column 4, lines 1-4), particularly where the credential, to be encrypted with the server's public key, contains the NetName of the client and a verifier including a time stamp (see Rosenthal, column 4, lines 19-23) resulting in a message represented outside the range of 0 to $(n - 1)$, where n is the product of two prime numbers, where the message requires a conventional blocking means to break the message into block words before encoding with the RSA public key encryption method (see Rivest et al., column 4, lines 33-37). Additionally, the credential directs the server to determine the authorization of the particular user that issued the credential (see Rosenthal et al., column 4, lines 17-32; the credential constructed by the client controlled by the user is sent to the server to determine the authorization of a particular user). The credential functions as a command, defined as an instruction to a computer program that, when issued by the user, causes an action to be carried out (see Microsoft Press Computer Dictionary, 3rd Ed., page 101).

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

Art Unit: 2132

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

7. Claims 31 and 32 are rejected under 35 U.S.C. 103(a) as being unpatentable over Rosenthal, U.S. Patent No. 5,073,933 A in view of Rivest et al., U.S. Patent No. 4,405,829 A.

As per claim 31, Rosenthal discloses an apparatus for controlling the execution by a machine of a trusted command that is issued by a user (see column 3, lines 58-67 and column 4, lines 1-32); the command of a user on a client to log onto to a server on an X Windows network-wide data base to determine the user's authorization; see Microsoft Press Computer Dictionary, 3rd Ed., page 101; where command is defined as an instruction to a computer program that, when issued by the user, causes an action to be carried out), comprising:

(a) untrusted parsing means for generating an encrypted command (see column 4, lines 17-23; a host implementing a client process to encrypt a credential with a server's public key containing the NetName of the client and a verifier including a time stamp; see column 4, lines 1-4; where the public key is given out by the server to persons whom he wishes to address messages to it so that they may encrypt the messages for his receipt only in a trusted manner; see column 4, lines 4-9; where the server is the only individual in possession of the secret key used to decrypt in a trusted environment the messages from untrusted hosts);

(b) means, readable by the machine, for causing the machine to receive the encrypted command from the untrusted encrypting means (see column 4, lines 24-26; the server receives the credential encrypted with the server's public key in a trusted manner from an untrusted host that the server decrypts with its secret key); and

(c) means, readable by the machine, for causing the machine to execute the trusted command (see column 4, lines 30-32; the server follows the user's instruction to determine the authorization of the particular user; column 5, lines 1-3; allowing the user who is logged in to talk to the server).

Although Rosenthal explains that the use of public key encryption is known in the art (see column 4, lines 10-16), he does not explicitly teach parsing.

Rivest et al. disclose public key encryption of a message by parsing (see column 4, lines 32-37; a conventional blocking means is utilized to break a message into block words before encoding by a program, where the message is represented by a number outside the range 0 to $(n - 1)$, where n is the product of two primes; see Microsoft Press Computer Dictionary, 3rd Ed., page 355; where parse is defined as to break input into smaller chunks so that a program can act upon the information).

Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the apparatus of Rosenthal with the parsing of Rivest et al. to implement public key encryption for transmission to a particular decoding device (see Rivest et al., column 4, lines 18-22; and see Rosenthal, column 4, lines 1-4), particularly where the credential, to be encrypted with the server's public key, contains the NetName of the client and a verifier including a time stamp (see Rosenthal, column 4, lines 19-23) resulting in a message represented outside the range of 0 to $(n - 1)$, where n is the product of two prime numbers, where the message requires a conventional blocking means to break the message into block words before encoding with the RSA public key encryption method (see Rivest et al., column 4, lines 33-37).

As per claim 32, Rosenthal discloses an apparatus for controlling the execution by a machine of a trusted command that is issued by a user with user identification data (see column 3, lines 58-67 and column 4, lines 1-32); the command of a user on a client to log onto to a server on an X Windows network-wide data base to determine the user's authorization including the NetName; see column 4, lines 30-32; indicative of a particular user; see column 4, lines 17 - 24; and a verifier encrypted with the user's (client's) secret key as a digital signature identifying the user; see Microsoft Press Computer Dictionary, 3rd Ed., page 101; where command is defined as an instruction to a computer program that, when issued by the user, causes an action to be carried out), comprising:

(a) untrusted parsing means for generating an encrypted command (see column 4, lines 17-23; a host implementing a client process to encrypt a credential with a server's public key containing the NetName of the client and a verifier including a time stamp; see column 4, lines 1-4; where the public key is given out by the server to persons whom he wishes to address messages to it so that they may encrypt the messages for his receipt only in a trusted manner; see column 4, lines 4-9; where the server is the only individual in possession of the secret key used to decrypt in a trusted environment the messages from untrusted hosts);

(b) means, readable by the machine, for causing the machine to receive the user identification data from the user (see column 4, lines 24-26; the server receives the credential; see column 4, lines 17-24; from the user through the host operating the client program including the NetName; see column 4, lines 30-32; indicative of a particular user; see column 4, lines 17 -

Art Unit: 2132

24; and a verifier encrypted with the user's (client's) secret key as a digital signature identifying the user);

(c) means, readable by the machine, for causing the machine to receive the encrypted command from the untrusted encrypting means (see column 4, lines 24-26; the server receives the credential encrypted with the server's public key in a trusted manner from an untrusted host that the server decrypts with its secret key); and

(d) means, readable by the machine, for causing the machine to perform a security check on the encrypted command (see column 4, lines 24-26; the server using its secret key to decrypt the credential; see column 4, lines 30-32; checking the credential against the network-wide database to determine the authorization of the particular user) and a security check on the user identification data (see column 4, lines 26-30; the server using the client's public key to decrypt the digital signature in the form of the verifier encrypted with the user's secret key where decryption by the client's public key identifies the user; see column 4, lines 51-56; and comparing the NetName with net names on an authorized list to allow a connection to the server); and

(e) means, readable by the machine, for causing the machine to execute the trusted command (see column 4, lines 30-32; the server follows the user's instruction to determine the authorization of the particular user; column 5, lines 1-3; allowing the user who is logged in to talk to the server).

Although Rosenthal explains that the use of public key encryption is known in the art (see column 4, lines 10-16), he does not explicitly teach parsing.

Art Unit: 2132

Rivest et al. disclose public key encryption of a message by parsing (see column 4, lines 32-37; a conventional blocking means is utilized to break a message into block words before encoding by a program, where the message is represented by a number outside the range 0 to $(n - 1)$, where n is the product of two primes; see Microsoft Press Computer Dictionary, 3rd Ed., page 355; where parse is defined as to break input into smaller chunks so that a program can act upon the information).

Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the apparatus of Rosenthal with the parsing of Rivest et al. to implement public key encryption for transmission to a particular decoding device (see Rivest et al., column 4, lines 18-22; and see Rosenthal, column 4, lines 1-4), particularly where the credential, to be encrypted with the server's public key, contains the NetName of the client and a verifier including a time stamp (see Rosenthal, column 4, lines 19-23) resulting in a message represented outside the range of 0 to $(n - 1)$, where n is the product of two prime numbers, where the message requires a conventional blocking means to break the message into block words before encoding with the RSA public key encryption method (see Rivest et al., column 4, lines 33-37).

Allowable Subject Matter

8. Claims 21-27, 29, 30, and 35-41 are allowed.
9. Claims 33 and 34 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Art Unit: 2132

10. The following is an examiner's statement of reasons for allowance:

Claims 21-26 and 35-41 are drawn to a method for verifying the existence of a trusted path to a user in a computing system. The closest prior art, Rosenthal et al., U.S. Patent No. 5,073,933 A, discloses a similar method. Rosenthal et al. teaches, upon login by a user (see column 4, lines 17-19; when a user logs on; see column 3, lines 25-27; on a client on the local host (physically at the server) to change the access control list), assigning a process identifier to the user in the trusted computing environment (see column 4, lines 57-67; column 5, lines 1-3; adding an entry of a new authorized NetName identifying a process forming a session between a user and a server) in response to a ChangeHost request with the family NetName (see column 4, lines 57-60). However, Rosenthal et al. neither shows nor motivates automatically assigning a process identifier to the user in the trusted computing environment. This distinct step explicitly recited in independent claim 21 renders claims 21-26 and 35-41.

Claims 27, 29, and 30 are drawn to an apparatus for executing a trusted command that is issued by a user. The closest prior art, Rosenthal, U.S. Patent No. 5,073,933 A in view of Rivest et al., U.S. Patent No. 4,405,829 A, describes a similar apparatus. Rosenthal et al. mentions a means for displaying a representation of the effect that a trusted encrypted command is intended to carry out to the user for verification (see column 5, lines 1-3; the user who has logged in is allowed to talk to the server which informs the host that the user has successfully logged on; see column 1, lines 55-56; displaying the successful login of a user on the monitor to the user). Neither Rosenthal et al. nor Rivest et al. explain displaying a representation of a trusted parsed command to the user for verification. This particular step explicitly recited in independent claim 27 renders claims 27, 29, and 30 allowable.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

11. The following is a statement of reasons for the indication of allowable subject matter:

Claim 33 is drawn to an apparatus for controlling the execution by machine of a trusted command. The closest prior art, Rosenthal, U.S. Patent No. 5,073,933 A in view of Rivest et al., U.S. Patent No. 4,405,829 A, disclose a similar apparatus. However, neither Rosenthal nor Rivest et al. teach or suggest a means, readable by the machine, for causing the machine to receive a signal from the user signifying whether the displayed representation accurately represents the trusted command; and a means, readable by the machine, for preventing the machine from executing the trusted command if the signal signifies that the parsed command does not accurately represent the trusted command. These composite features explicitly recited in dependent claim 33 render it to have allowable subject matter.

Claim 34 is drawn to an apparatus for controlling the execution by machine of a trusted command. The closest prior art, Rosenthal, U.S. Patent No. 5,073,933 A in view of Rivest et al., U.S. Patent No. 4,405,829 A, disclose a similar apparatus. However, neither Rosenthal nor Rivest et al. teach or suggest a means, readable by the machine, for causing the machine to receive a signal from a second user signifying whether the displayed representation accurately represents the trusted command; and a means, readable by the machine, for preventing the machine from executing the trusted command if the signal signifies that the parsed command

Art Unit: 2132

does not accurately represent the trusted command. These composite features explicitly recited in dependent claim 34 render it to have allowable subject matter.

Conclusion

12. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the mailing date of this final action.

Telephone Inquiry Contacts

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Justin T. Darrow whose telephone number is (571) 272-3801, and whose electronic mail address is justin.darrow@uspto.gov. The examiner can normally be reached Monday-Friday from 8:30 AM to 5:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barrón, Jr., can be reached at (571) 272-3799.

The fax number for Formal or Official faxes to Technology Center 2100 is (703) 872-9306. In order for a formal paper transmitted by fax to be entered into the application file, the paper and/or fax cover sheet must be signed by a representative for the applicant. Faxed formal papers for application file entry, such as amendments adding claims, extensions of time, and statutory disclaimers for which fees must be charged before entry, must be transmitted with an authorization to charge a deposit account to cover such fees. It is also recommended that the cover sheet for the fax of a formal paper have printed "**OFFICIAL FAX**". Formal papers transmitted by fax usually require three business days for entry into the application file and consideration by the examiner. Formal or Official faxes including amendments after final rejection (37 CFR 1.116) should be submitted to (703) 872-9306 for expedited entry into the application file. It is further recommended that the cover sheet for the fax containing an amendment after final rejection have printed not only "**OFFICIAL FAX**" but also "**AMENDMENT AFTER FINAL**".

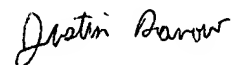
Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications

Art Unit: 2132

may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (571) 272-2100.

May 28, 2005



**JUSTIN T. DARROW
PRIMARY EXAMINER
TECHNOLOGY CENTER 2100**